Documents to be included in the AISA Training Binder:

Top Vulnerabilities-

Compliance Issues

This document comprises a summary of the types of records exempt from the Public Records Act and information protected under the Information Practices Act. The types of confidential information most likely to be included in CDC's information systems are:

- Personal information, defined in the Civil Code, Information Practices Act, section 1798 (in particular, SSN, CDL/ID Card Numbers, Bank Accounts and Credit Card numbers).
- Health and medical records.
- Health contracts and related information, including hospital and patient services, and health and medical maintenance.
- Investigatory or security documents from or to law enforcement agencies, correctional agencies or for licensing purposes.
- Information collected under the Evidence Code.
- Correspondence with the Governor or his office.
- Documents pertaining to collective bargaining
- Vulnerability assessments related to terrorism and other criminal activity.
- Test questions pertaining to employment examinations.
- Documents pertaining to pending litigation.

In addition, the Penal Code, Section 11075, requires that we maintain confidentiality of Criminal offender record information (CORI data).

What is NOT confidential?

- Information recorded in the County Recorder's Office
- Names
- CDC Numbers
- Fictitious Business Names

Department of Corrections and Rehabilitation
Statement of Agreement to Responsibilities and Usage of Data Received

Receiving Organization: _____

California State Government ____ Yes ____ No

Description of Data Set:

Description of the intended usage:

Transmittal Method:

____ FTP ____ Hardcopy ____ Tape
____ CD ____ Removable Media
____ E-mail ____ Other (please describe _____)

Frequency of Transmittal:

_____ One-time _____ Weekly _____ Monthly
_____ Annually _____ Other (please describe _____)

Does this data set include confidential information? ____ Yes ____ No
If yes, the data set will be encrypted if it is transmitted across the Public Internet.

Confidential information may not be transmitted using email. (Dom, Sections 49020.20.3).

Usage of this dataset is limited in the following ways:

1. The dataset may be used ONLY for the purpose described above.
2. This dataset may NOT be shared with any other entity for any reason without prior written approval from CDC.
3. The dataset must be stored in such a manner as to provide for its protection at the same level it is protected by CDC. This includes the following provisions:
   a. All appropriate security patches, virus protection software and system upgrades must be current on the computer(s) used to store or access this dataset.
   b. Access to the dataset must be limited by appropriate permissions and authorizations.
4. In the event that the dataset is accessed by unauthorized staff or is otherwise compromised or believed to be compromised, the CDC Information Security

Officer must be notified promptly. Notification information is located on the reverse side of this form.

5. If the dataset includes confidential data elements, non-disclosure forms must be signed by all staff in your organization with access to this information.

Receiving Organization

I agree to abide by these terms and conditions, and to ensure that all staff with access to this dataset also abide by these terms and conditions:

Signature	Print Name	Date
Title		

CDC Data Owner Authorization

I understand that the dataset described above is to be shared with the indicated organization for the stated reason. Transmittal and sharing of this information to the so indicated organization is approved and authorized.

Signature	Print Name	Date
Title		

CDC Data Custodian Acknowledgement

Signature	Print Name	Date
Title		

CDC Information Security Officer contact information.

Information Security Officer
Department of Corrections
PO Box 942883
Sacramento CA 94283-0001

916-358-2459
debborah.martin@corr.ca.gov

User Agreement Forms

CDC Form 3025 (see separate file)
CDC Form 1900 (see separate file)
CDC Form 1857 (see separate file)

Incident Reporting

49020.7 Reportable Incident Criteria

It is the responsibility of all departmental employees to report all incidents that would place the Department's information assets at risk. The following incidents shall be reported through the local ISC and chain of command to the Chief Deputy Directors and to the departmental ISO within three days of becoming aware that an incident has occurred:

- Unauthorized access to, or modification of, State-owned or State-managed data, including nonelectronic data such as reports, documentation, and hard copy files.
- Unauthorized use of, or access to, State computer resources, including computer networks and services, as well as systems not necessarily connected to a network.
- Unauthorized access to, or modification of, computer software, including operating systems, networks, configurations and applications. This includes the introduction of malicious software such as viruses, worms, and other malicious software.
- Deliberate or unauthorized acts resulting in disruption of State computer services, including "Denial of Service" attacks.
- Unauthorized use of user account or Internet domain names.
- Destruction of, or damage to, State information processing facilities.
- Break-in or other unauthorized access to State facilities resulting in compromise to the data or computer systems housed within those facilities.

CDC management shall investigate all incidents.

Incident Reporting Template

(see separate file)

Email

See the Email Guide, separate file

Non-CDC Devices and Software

(see separate file)